3GPP TSG CN Plenary Meeting #12 **Tdoc NP-010361**
Stockholm, Sweden, 13th - 15th June 2001

Source: TSG CN WG4

Title: CRs on Rel-5 Work Item SS7IP

Agenda item: 9.13

Document for: Information

Introduction:

This document contains 1 TR on Rel-5 Work Item ”SS7IP”, that have been agreed by TSG CN WG4, and are forwarded to TSG CN Plenary meeting #12 for information.

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
29.903			N4-010666	Rel-5	3GPP TR 29.903 Version 0.1.0 Feasibility Study on SS7 Signalling		0.1.0

3GPP TR 29.903 V0.1.0 (2001-06)

Technical Report

3rd Generation Partnership Project (3GPP);
Technical Specification Group Services and System Aspects;
Feasibility Study on SS7 signalling transport in the core network with SCCP-User Adaptation Layer (SUA)
(Release 5)

Keywords

3GPP, CN4, SUA, SS7, Sigtran

3GPP

Postal address

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Figures

Foreword

This Technical Report has been produced by the 3GPP.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TR, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

Where:

x is the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 Indicates TSG approved document under change control.

y is the second digit incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z is the third digit incremented when editorial only changes have been incorporated in the specification.

1 Scope

The scope of this Technical Report (TR) is to capture the results of a feasibility study on SS7 signalling transport (e.g. MAP & CAP) in a 3GPP core network with SCCP-User Adaptation (SUA) for Release-5.

With this purpose in mind, this TR evaluates the advantages and disadvantages associated with the implementation of SUA in the core network, and compares it with the SCCP/M3UA option. Therefore, an overview of M3UA is provided in this document for reference. This TR covers all scenarios such as SUA peer to peer as well as interworking with legacy SS7 network, plus the interworking between SUA and SCCP/M3UA. This TR also identifies and studies the technical issues related to SUA implementation and proposes the possible technical solutions that will enable the efficient implementation of SUA, with minimum impacts on the available services.

More generally, the aim of this TR is to identify and strive to solve all issues introduced by such evolution of the core network signalling. At the end of the feasibility study, the open issues are reported and their importance is assessed. Also discussed are the benefits and drawbacks with respect to the introduction of SUA into 3GPP core network signalling.

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative References

[1] 3GPP TS 21.905: “3G Vocabulary”

[2] 3GPP TS 29.202: “SS7 Signalling Transport in Core Network; Stage 3”

[3] 3GPP TS 29.002: “Mobile Application Part (MAP) specification”

[4] 3GPP TS 29.078: “Customised Applications for Mobile network Enhanced Logic; (CAMEL) Phase 3; CAMEL Application Part (CAP) specification”

[5] 3GPP TS 29.013: "Signalling interworking between ISDN supplementary services; Application Service Element (ASE) and Mobile Application Part (MAP) protocols"

[6] 3GPP TS 29.066: " Support of Mobile Number Portability (MNP); Technical Realisation "

[7] 3GPP TS 33.200 “Network Domain Security”

[8] IETF RFC 2960: Stream Control Transmission Protocol (SCTP)

http://www.ietf.org/rfc/rfc2960.txt

[9] IETF INTERNET-DRAFT: SS7 SCCP-User Adaptation Layer (SUA)

http://www.ietf.org/internet-drafts/draft-ietf-sigtran-sua-05.txt

[10] IETF INTERNET-DRAFT: SS7 MTP3-User Adaptation Layer (M3UA)

http://www.ietf.org/internet-drafts/draft-ietf-sigtran-m3ua-06.txt

[11] IETF RFC 2916: E.164 number and DNS (ENUM)

http://www.ietf.org/rfc/rfc2916.txt

[12] IETF RFC 1034 Domain Names –Concepts and Facilities

http://www.ietf.org/rfc/rfc1034.txt

[13] IETF RFC 1035 Domain Names –Implementation And Specification

http://www.ietf.org/rfc/rfc1034.txt

[14] IETF RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record

http://www.ietf.org/rfc/rfc2915.txt

2.2 Informative References

[15] IETF RFC 2719: Framework Architecture for Signalling Transport

http://www.ietf.org/rfc/rfc2719.txt

[16] ITU-T Recommendation E.164: "Numbering plan for the ISDN era"

[17] ITU-T Recommendation E.212: "Identification plan for land mobile stations"

[18] ITU-T Recommendation E.214: "Structuring of the land mobile global title for the signalling connection control part"

[19] ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Functional description of the Signalling Connection Control Part".

[20] ITU-T Recommendation Q.712: "Definition and function of SCCP messages".

[21] ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; SCCP formats and codes".

[22] ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling Connection Control Part procedures".

[23] ANSI T1.112 (1996): "Telecommunication – Signalling No. 7 – Signaling Connection Control Part (SCCP)"

3 Definitions and Abbreviations

3.1 Definitions

IPSP: Signalling Point in the IP network

Mobile Number: In this document the expression “Mobile Number” is used to indicate any of the E.164, E.212 and E.214 numbers of the mobile.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASP	Application Server Process
AP	Application level protocol (SCCP User Protocols)
AS	Application Server
BG	Border Gateway
AAL5	ATM Adaptation Layer type 5
ATM	Asynchronous Transfer Mode
CAMEL	Customized Application for Mobile Network Enhanced Logic
CAP	CAMEL Application Part
CC	Country Code
NDC	National Destination Code
CCBS	Call Completion to Busy Subscriber
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service

GTT	Global Title Translation
HPLMN	Home Public Land Mobile Network
VPLMN	Visitor Public Land Mobile Network
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
IWF	Interworking Function
M3UA	MTP3-User Adaptation
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MNP	Mobile Number Portability
MTP	Message Transfer Part
MTP1	Message Transfer Part layer 1
MTP2	Message Transfer Part layer 2
MTP3	Message Transfer Part layer 3
NAPTR	The Naming Authority Pointer
MTU	Maximum Transfer Unit
NPDB	Number Portability Database
PDH	Plesiochronous Digital Hierarchy
RANAP	Radio Access Network Application Part
RNSAP	Radio Network Subsystem Application Part
SMMT	Short Message Mobile Terminated
SMMO	Short Message Mobile Originated
SMS	Short Message Service
SSAP	Supplementary Service Application Part
SSCF	Service Specific Coordination Function
SSCOP	Service Specific Connection Oriented Protocol
SCCP	Signalling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SUA	SCCP-User Adaptation layer
T-BCSM	Terminating Basic Call State Model
TC	Transaction Capabilities
TCAP	Transaction Capabilities Application Part
TPDU	Transfer Protocol Data Unit
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Indentifiers

4 Introduction

The purpose of this technical report (TR) is *i)* to discuss the advantages and disadvantages of using the SUA protocol to transport MAP and/or CAP signalling over an IP based core network, and *ii)* to propose SUA as an alternative option for MAP/CAP transport in Rel5.

5 SUA Overview

SCCP-User Adaptation (SUA) is a new protocol, currently developed by IETF (see draft-ietf-sigtran-sua-05.txt), for the transport of any SS7 SCCP-User signalling (e.g. TCAP etc.) over IP using the Stream Control Transport Protocol (SCTP). SUA aims to be modular and symmetric, to allow it to work in diverse architectures, such as a Signalling Gateway to IP Signalling Endpoint architecture as well as a peer-to-peer IP Signalling Endpoint architecture.

5.1 Sigtran Background

Stream Control Transmission Protocol (SCTP), defined by the Signal Transport (SIGTRAN) working group of the Internet Engineering Task Force (IETF), is a transport level datagram transfer protocol that operates on top of an unreliable datagram service, such as Internet Protocol (IP). Like TCP, SCTP provides a reliable transport service, ensuring that data is transported across the network without error and in sequence. SCTP works on the basic concepts of associations and streams. An SCTP association is similar to a TCP connection, except it can support multiple IP addresses at either or both ends. An SCTP association is comprised of multiple logical streams, ensuring the sequenced delivery of user messages within a single stream. SCTP achieves the reliable message transport service by retransmitting lost messages similar to what TCP does. However, unlike TCP, the retransmission by SCTP of a lost message in one stream does not block the delivery of messages in other streams. The use of multiple streams within SCTP resolves the issue of head-of-line blocking associated with the use of TCP. The basic SCTP functionality includes:

- Acknowledged error-free non-duplicated transfer of data streams
- Data fragmentation to conform to Message Transfer Unit (MTU) size
- Sequenced delivery of user messages within multiple streams with an option for order of arrival and?? delivery of individual user messages
- Bundling of multiple user messages into a single SCTP packet
- Network level fault tolerance due to the support of multi-homing at either or both ends of an association

The SCCP-User Adaptation Layer (SUA), defined by the SIGTRAN working group of the Internet Engineering Task Force (IETF), transports signalling messages from SCCP users, such as Transaction Capabilities Application Part (TCAP), Radio Access Network Application Part (RANAP) and Radio Network Subsystem Application Part (RNSAP), over the Internet Protocol (IP) network, using the Stream Control Transmission Protocol (SCTP). SUA allows the seamless interoperation between SCCP users in the SS7 and IP domains. RANAP and RNSAP transport and their associated protocol stacks are being studied by the “IP Transport in UTRAN” work item in the RAN3 working group.

5.2 SUA Functionality

The SUA delivery mechanism provides the following functionality:

- Support for transfer of SS7 SCCP-User Part messages;
- Support for SCCP connectionless service;
- Support for SCCP connection oriented service;
- Support for the seamless operation of SCCP-User protocol peers;
- Support for the management of SCTP transport associations between a Signalling Gateway and one or more IP-based signalling nodes to the degree specified by the SCCP user application;
- Support for distributed IP-based signalling nodes; and
- Support for the asynchronous reporting of status changes to management.

5.3 Mapping Between SCCP Messages and SUA Messages

For the seamless support transfer of SCCP-User Part messages, all SCCP messages can be mapped into associated SUA messages.

SUA	**SCCP**	**SCCP**	**Classes**				**Mgt.**	**SUA**
NAME	**NAME**	**Full Name**	**0**	**1**	**2**	**3**	**Msg.**	**Usage**
		Connectionless Messages						
CLDT	UDT	Unitdata	x	x	-	-	-	-
CLDT	XUDT	Extended unitdata	x	x	-	-	-	-
CLDT	LUDT	Long unitdata	x	x	-	-	-	-
CLDR	UDTS	Unitdata service	x	x	-	-	-	-
CLDR	XUDTS	Extended unitdata service	x	x	-	-	-	-

CLDR	LUDTS	Long unitdata service	x	x	-	-	-	-
		Connection-Oriented Messages						
CODT	DT1	Data form 1	-	-	x	-	-	-
CODT	DT2	Data form 2	-	-	-	x	-	-
CODT	ED	Expedited data	-	-	-	x	-	-
CODA	AK	Data acknowledgement	-	-	-	x	-	-
CODA	EA	Expedited data acknowledge	-	-	-	x	-	-
CORE	CR	Connection request	-	-	x	x	-	-
COAK	CC	Connection confirm	-	-	x	x	-	-
COAK	CREF	Connection refused	-	-	x	x	-	-
RELRE	RLSD	Released	-	-	x	x	-	-
RELCO	RLC	Release complete	-	-	x	x	-	-
RESRE	RSR	Reset request	-	-	-	x	-	-
RESCO	RSC	Reset confirm	-	-	-	x	-	-
COIT	IT	Inactivity test	-	-	x	x	-	-
COERR	ERR	Protocol Data Unit Error	-	-	x	x	-	-
		SS7 MGT Messages						
DUNA	n/a	n/a	-	-	-	-	-	x
DAVA	n/a	n/a	-	-	-	-	-	x
DAUD	n/a	n/a	-	-	-	-	-	x
SCMG	SSC	SCCP/subsystem-congested	-	-	-	-	x	-
SCMG	SSA	Subsystem-allowed	-	-	-	-	x	-
SCMG	SSP	Subsystem-prohibited	-	-	-	-	x	-
SCMG	SST	Subsystem-status-test	-	-	-	-	x	-
SCMG	SOR	Subsystem-oos-req	-	-	-	-	x	-
SCMG	SOG	Subsystem-oos-grant	-	-	-	-	x	-
		SUA MGT Messages						
ASPUP	n/a	n/a	-	-	-	-	-	x
ASPDN	n/a	n/a	-	-	-	-	-	x
ASPAC	n/a	n/a	-	-	-	-	-	x
ASPIA	n/a	n/a	-	-	-	-	-	x
NTFY	n/a	n/a	-	-	-	-	-	x
ERR	n/a	n/a	-	-	-	-	-	x

SUA messages (CLDT, CLDA) support all 6 SCCP connectionless messages.

```
-   = Message not applicable for this protocol class.
X   = Message applicable for this protocol class.
n/a = not applicable
```

5.4 Status in IETF

At the present time, SUA is still under development by the SIGTRAN Working Group in IETF. The latest version is 5. It is expected to be on last call for the next revision, which is schedule to be released soon.

6 M3UA Overview

In order to compare SUA and M3UA, it is necessary to give a brief introduction of M3UA and its implementation and its adoption in 3GPP in this technical report.

MTP3-User Adaptation (M3UA) is a protocol, currently developed by IETF[10], for the transport of any SS7 MTP3-User signalling (e.g. ISUP, SCCP, and TUP.) over IP using the Stream Control Transport Protocol (SCTP). M3UA can also work in diverse architectures, such as a Signalling Gateway to IP Signalling Endpoint architecture as well as a peer-to-peer IP Signalling Endpoint architecture.

6.1 M3UA Functionality

The M3UA delivery mechanism provides the following functionality:

- Support for transfer of SS7 MTP3-User Part messages;
- Support for the management of SCTP transport protocol between a Signalling Gateway and one or more IP-based signalling nodes to ensure transport availability to MTP3 user signalling applications;
- Support for the seamless operation of MTP3-User protocol peers;
- Support for distributed IP-based signalling nodes; and
- Support for the asynchronous reporting of status changes to management.

6.2 M3UA Implementation

The usage of M3UA to transport MAP and TCAP messages is illustrated in Figure 1.

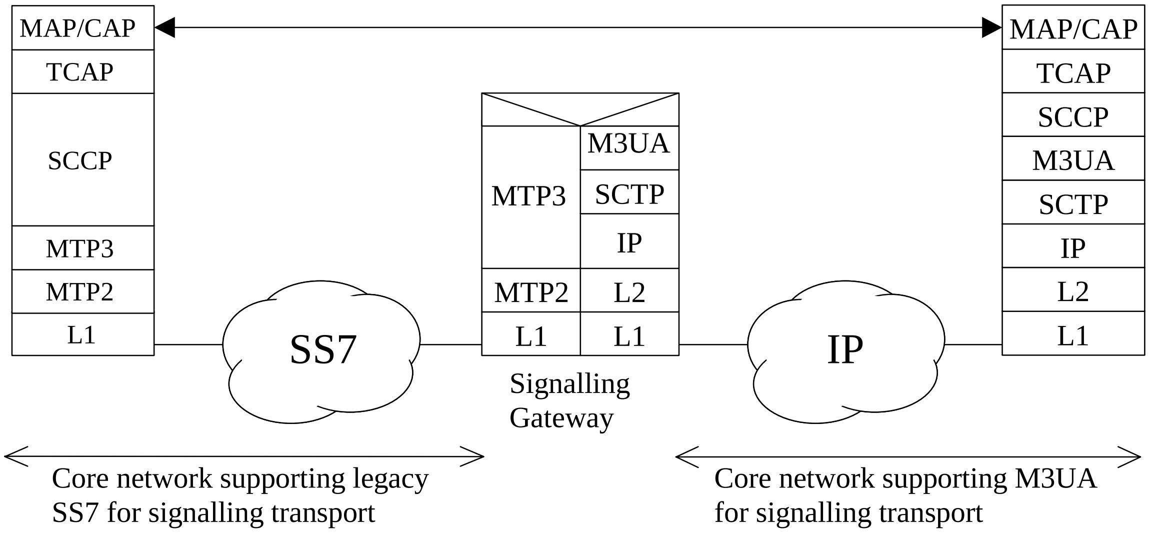
MAP/CAP
TCAP
SCCP
MTP3
MTP2
L1
SS7
MTP3
M3UA
SCTP
IP
MTP2
L2
L1
L1
Signalling Gateway
IP
MAP/CAP
TCAP
SCCP
M3UA
SCTP
IP
L2
L1
Core network supporting legacy SS7 for signalling transport
Core network supporting M3UA for signalling transport

Figure 1: Transportation of MAP and CAP via M3UA

An example of SCCP transport between IPSPs is illustrated in Figure 2. SCCP messages are exchanged directly between two IP resident IPSPs with SCCP user protocol like TCAP, RANAP and RNSAP.

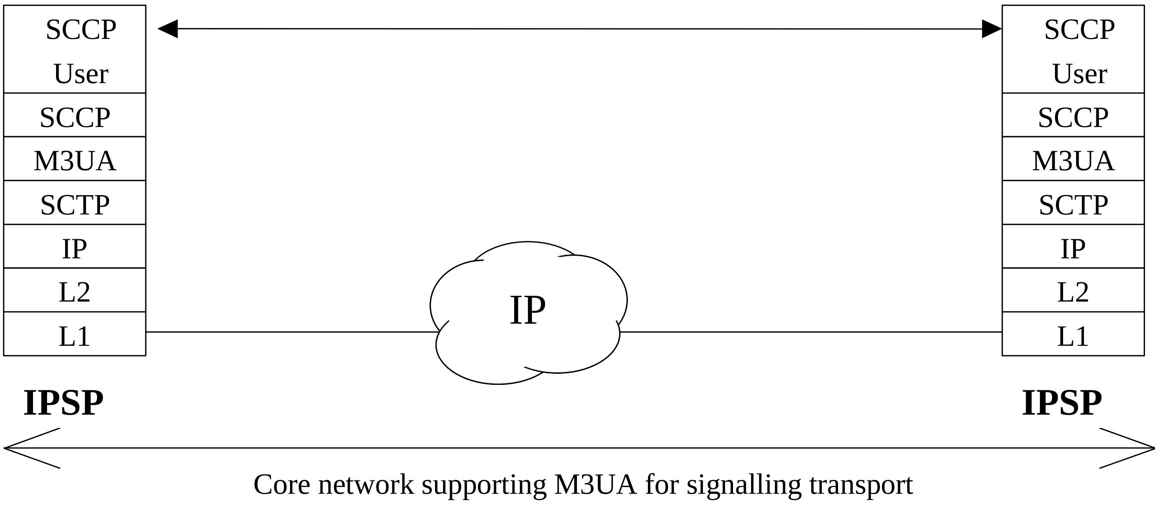

Figure 2: Transportation of SCCP-user messages via M3UA in all IP network

6.3 M3UA Adoption in 3GPP

Please refer to 3GPP TS 29.202[1] for transporting MAP & CAP messages in a 3GPP core network using M3UA. Meanwhile, M3UA is specified as an option for RANAP in 3GPP TS 25.412 and RNSAP in 3GPP TS 25.422 to transport SCCP messages in a packet switched domain.

7 SUA Implementation

The transport of the signalling protocols which can be identified as SCCP-users, such as TCAP, RANAP and RNSAP, and in turn the transport of TCAP-users such as MAP and CAP, shall be accomplished in accordance with the defined protocol architectures defined in the following sub-clauses.

SUA transports any SS7 SCCP user signalling messages over IP using SCTP between two signalling endpoints. The protocol is able to work in diverse architectures such as an SG to IP signalling endpoint architecture as well as a peer-to-peer IP signalling endpoint architecture. This support allows SUA to carry a protocol that uses the transport services of SCCP, but is contained within an IP network. Depending upon the upper layer protocol supported, the SUA will need to support SCCP connectionless service, SCCP connection oriented service or both services.

7.1 SUA In an All IP Environment

SUA allows extra flexibility in developing networks, especially when interaction between legacy systems is not needed.

SUA, apart from carrying SCCP-User protocols, can also provide Address Mapping Function (AMF) to route the messages to the next or destination node. The Address Mapping Function, apart from the translations providing the GTT services defined for SS7 networks, modelled in [ITU-T Q.714], also provides the following translations

- Global Title Information + optional SSN To IP Address
- Host Name + optional SSN To IP Address

SUA, with the additional translation capabilities provided by AMF, can now route the messages to nodes within an IP network. AMF can be implemented as part of SUA or can be implemented as a separate process accessible to the SUA. Even in the case of AMF being a separate process, it should be considered as a service provided by the SUA.

SUA can provide the mapping service through various approaches such as local table lookup or external database access (e.g. ENUM servers) as well as their combination as described below. Please note that the terms ENUM and DNS can be used interchangeably.

a) Only Local Tables. This option will not be feasible to support Inter-PLMN signalling, and so will not be explained further in this report.

b) Only ENUM Servers. One could store all the numbers in the ENUM servers (E.164 and E.212). This option requires IETF to define standards to store E.212 numbers in the ENUM server This requires further study.

c) Both local tables and ENUM server. In this option ENUM servers will be accessed only if mapping cannot be performed using the data from local tables.

It should be noted that the procedures for updating the local tables is implementation dependent and will not be further standardised. With the introduction of SUA in a 3GPP core network, the routing of SCCP-User messages in the IP network can be achieved using either existing ENUM servers (if operators already have ENUM servers) or deploying new ENUM servers that can be used for more than one purpose. So, the investment made by the operator for the purpose of SUA is well protected, since the hardware and the data can be used for future IP based services (e.g. SIP based multimedia services).

The Address Mapping Function will be invoked when the routing indicator of the Called Party Address Field is set to:

- Routing is on Global Title
- Routing is on Hostname

Input to the Address Mapping Function shall be one of the following

- Global Title Information which includes E.164 number, E.212 number and E.214 number. (Distinction among different numbering plans can be made by looking at the 'Global Title' field of the Called Party Address) + optional SSN
- Host Name + optional SSN
- IP Address + SSN

Note: SSN number is required by SUA to identify the service requested by the upper application layers.

The output of the Address Mapping Function shall be one of the following:

- Route on GT: SCTP association ID towards the Signalling Gateway (SG) + (new) GT + optional SSN + Network Appearance (Optional)
- Route on SSN: SCTP association ID towards the destination node + SSN + Network Appearance (Optional)

7.1.1 Architecture

As described above, SUA locates the next or destination IP node through the Address Mapping Function. It is also mentioned that the Address Mapping Function can be provided using a combination of local tables and ENUM server. In the architecture we also show the presence of Signalling Gateways at the border of the PLMN. As we will see in the later sections, in certain cases, the Signalling Gateway acts as a relay point for messages flowing to/from the PLMN. In such cases, the SUA messages will be routed by the SG to the destination SUA node based on the GT information or some other means, for example TCAP transaction ID.

In a scenario where the ENUM severs can support and handle E212 numbers, the originating node can communicate with the ENUM server without going through the Signaling gateway (SG). The SG may be required for other reasons such as security, interfacing with a legacy SS7 network and so on.

Figure 3 shows the possible realisation of the architecture.

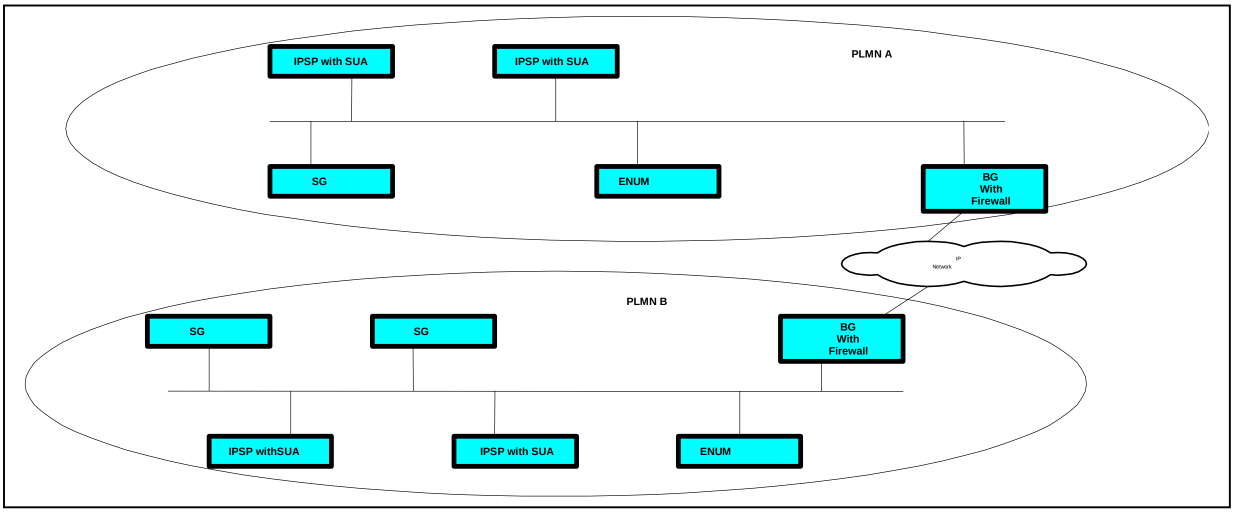

Figure 3: SUA implementation in an all IP network

ENUM servers within the PLMN can contain the local E.164 numbers in the form of domain names along with the supported service names and their location. The structure and format of the ENUM record should conform to RFC 2916 spec. Each record in the ENUM server can either represent a single subscriber or a group of subscribers (using wild cards). Along with the E.164 records, the ENUM server shall also contain one record for the domain name corresponding to all the E.212 numbers belonging to a PLMN (*This option is proposed to avoid the need to create a new domain for E.212, for example e212.arpa*). This domain name has to be constructed from the *CC* and *NDC* or *an Equivalent Number* values assigned to that PLMN, the *CC* is derived from *MCC*. To avoid collisions we can standardise the format for the domain described above. For example the format can be *imsi.<cc>.<ndc>.e164.arpa*. (Please note the *imsi* is a lable not the value.) The IP address or the host name corresponding to the domain name described above should be one of the following

- IP address of the SG acting as a relay point for the PLMN

- Host name corresponding to a pool of SGs in case of more than one SG (For load sharing and redundancy) in the PLMN.

The scheme used for E.212 number can be used for any other Global Titles (current or future)

SUA nodes in the above figure could be provided with the local tables to perform the Address Mapping Function. For efficiency, the information in the local tables and local ENUM server (*Note: ENUM server now can be used only to store E.164 numbers*.) should be sufficient to provide intra-PLMN routing. SUA shall be able to perform the following translations.

a) Global Title + optional SSN to IP Address

b) Host Name + optional SSN To IP Address

When local tables are provided, query to the external ENUM server is only required in the Inter-PLMN case.

ENUM servers from different PLMNs are connected through referrals (a referral is an address to another ENUM server) using an approach similar to the one used to link existing DNS servers (see RFC 1034 and RFC 1035).

7.1.2 Routing SUA Messages in an Inter-PLMN Environment.

As mentioned above, each SUA node can be provided with local tables containing necessary information for routing the messages within the PLMN. However, it is not feasible for the SUA to have the information from other PLMNs. In such cases it has to rely on the services provided by the ENUM for routing the message to the node in a different PLMN.

Two scenarios will be considered in this report to explain the process involved in routing the messages between SUA nodes from different PLMNs..

0 Routing using provided E.164 (MSISDN) number.

1 Routing using provided E.212 (IMSI) number.

The two scenarios are explained in detail in the following sub-clauses.

7.1.2.1 Routing Using Provided E.164 (MSISDN) Number

The following steps illustrate the process involved in routing the SUA messages using provided E.164 (MSISDN) number.

1. The SUA receives the E.164 number and SSN from its upper layers (In Called Party Address parameter)

2. The SUA with the AMF attempts to map the E.164 number + SSN to an IP address. Because the number is for the subscriber from a different PLMN, it cannot find a mapping IP address.

3. The SUA then constructs the domain name from the E.164 number and send a DNS query to the local ENUM server for the URIs associated with the constructed domain name. The ENUM server, by following the referrals, forwards the original query to the Authorised ENUM server (ENUM server in the target PLMN). The Authorised Name server either returns a list of IP addresses or URIs associated with the domain name (constructed from E.164 number) or an error code. The result isthen be forwarded to the SUA. Recall that the returned IP address or URI is for the destination SUA node and not the SG (no need to go through the SG). URIs will be resolved with IP addresses.

4. From the list of IP addresses returned, the SUA has to pick the IP address associated with the service represented by the SSN.

5. The SUA message is sent to the IP address found in Step 4. The destination SUA node routes the message to the application identified by the SSN in the Called Party Address parameter.

Since DNS queries across PLMNs can sometimes take a while, the following enhancements are recommended to improve system performance:

a) Local ENUM servers or SUA nodes cache the information so subsequent queries need not cross PLMN boundaries. Caching remote DNS data is a standardised mechanism in DNS service. However, care should be taken to invalidate the cache after TTL expires (TTL is returned as part of DNS result). Applications should also be able to handle error conditions (Cache pointing to an invalid node) and re-request the data.

b) ENUM server lookup to be performed by the SG. In this case, if the originating SUA node cannot find an entry in its local lookup tables it has to forward the SUA message to a SG within the PLMN. Selection of the SG is implementation dependent.

7.1.2.2 Routing Using Provided E.212 (IMSI) Number

The following steps illustrate the process involved in routing the SUA messages using the provided E.212 (IMSI) number.

1) The SUA receives E.212 number and SSN from its upper layers (In Called Party Address parameter)

2) The SUA with the AMF attempts to map the E.212 number + SSN to an IP address. Because the number is for the subscriber from a different PLMN, it may not find a mapping IP address if the data is not cached after ENUM request or the caching expired.

3) The SUA then extracts the *MCC* and *MNC* values from the E.212 number. In order to hide the IMSI structure, *CC* and *NDC* (Part of E.164 number) should be derived from *MCC* and *MNC* values.

4) The SUA will construct the domain name from the derived *CC* and *NDC* values. The domain name will be of the form imsi.<CC>.<NDC>.e164.arpa. A DNS query will be sent to the local ENUM server to retrieve the URI, in the form of x@hostname or y@ipaddress, associated with the domain constructed above. URIs will be resolved with IP addresses.

5) The ENUM server, by following the referrals, forwards the original query to the Authorised ENUM server. The Authorised Name server either returns a list of URIs associated with the domain name or an error code. The result isthen be forwarded to the SUA. Recall that the address returned by the ENUM server will be one of the following:

a) IP address of the SG of the target PLMN

b) Host name corresponding to a pool of SGs in case of multiple SGs in the target PLMN (for redundancy and load sharing).

6) Send the SUA message to the IP address received in Step 5. The message will be sent with the following information:

  - Routing Indicator Set to Route on GT:
  - Address Parameter with Global Title (Converted from E.212 to E.214) and SSN

7) When the SG at the destination PLMN receives the message it will look up its internal table to derive the destination SUA node's IP address from the Global Title and SSN information of the SUA.

8) A message will be sent to the destination SUA node. The destination SUA node routes the message to the application identified by the SSN in the Called Party Address parameter.

Because DNS queries across PLMNs can sometimes take several seconds, the following alterations are recommended to improve system performance:

a) Local ENUM servers or SUA nodes cache the information so subsequent queries need not cross PLMN boundaries. Caching remote DNS data is a standardised mechanism in DNS service. However, care should be taken to invalidate the cache after TTL expires (TTL is returned as part of the DNS result). Applications should also be able to handle error conditions (Cache pointing to an invalid node) and re-request the data.

b) ENUM server lookup is to be performed by the SG. In this case, if the origination SUA node cannot find a matching entry in its local tables, it has to forward the SUA message to a SG within the PLMN. Selection of the SG is implementation dependent.

7.1.3 Security Considerations

As this solution is built on top of DNS, it will not be any more secure than today's DNS solution. Use of firewalls and other security measures are required to prevent unauthorized access to the ENUM servers located inside the PLMN. The BG shown in **Figure 3** can provide the security.

7.1.4 IANA Consideration

The values for the services applicable for Mobile Networks, for example HLR, VLR etc., may need to be standardised. These values must be specified in a published specification and approved by the IESG. The syntax for the service field value is defined in RFC 2915.

7.1.5 Message Segmentation

In an all IP environment, SCTP is responsible for fragmenting the SUA messages. When needed, SCTP fragments user messages to ensure that the SCTP packet passed to the lower layer conforms to the path MTU. On receipt, fragments are reassembled into complete messages before being passed to the SUA layer.

7.2 Interworking with Legacy SS7 Network

When interworking between SS7 and IP domains is needed, the SG (Signalling Gateway) acts as the gateway node between the SS7 network and the IP network. The SG will transport the SCCP-User signalling traffic from the SS7 network to the IP-based signalling node and vice-versa.

7.2.1 Architecture

Figure 4 illustrates an architecture that carries an SS7 application protocol (e.g. RANAP, TCAP) between an IP network and an SS7 network.

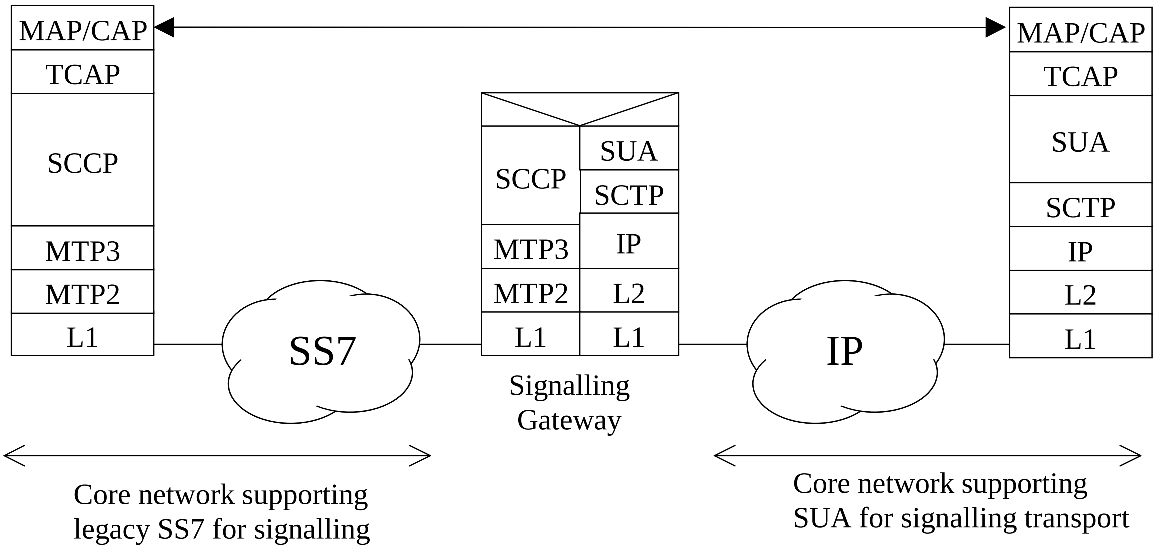
MAP/CAP
TCAP
SCCP
MTP3
MTP2
L1
SS7
SCCP
SUA
SCTP
IP
MTP3
MTP2
L2
L1
L1
Signalling Gateway
IP
MAP/CAP
TCAP
SUA
SCTP
IP
L2
L1
Core network supporting legacy SS7 for signalling
Core network supporting SUA for signalling transport

Figure 4: SS7 to IP Architecture via SUA

7.2.2 Global Title Management

In a heterogeneous network environment, where multiple IP networks are interconnected with SS7 networks, it is possible that the originating node does not know whether the destination signalling point is in the IP domain or in the SS7 domain. So it is possible that the originating signalling node shall use the services of a gateway to route the message to the destination. Hence, the gateway (*Note: This gateway can be a SG or a separate entity*) providing the GTT services should be able to determine, based on Global Title, the location of the destination (IP or SS7), and route the message to the appropriate entity.

7.2.3 Message Segmentation

The fragmentation and assembly on the IP side is handled by the SCTP. For messages, from and to the SS7 networks, message segmentation is provided by the SCCP layer at the SG.

7.3 Interworking with SCCP/M3UA

This is very similar to the case when interworking with SCCP/MTP3 in a legacy SS7 network. As illustrated in **Figure 5** below, the interworking could be implemented via an IWF that effectively relays the signalling messages across the two networks with incompatible signalling transports. In this case, all the SCCP-user messages carried across the two networks pass through the IWF. The IWF features an adaptation function on top of SCCP and SUA, which relays messages between these two protocols. The adaptation function of the IWF could be implementation specific and need not to be standardized.

7.3.1 Architecture

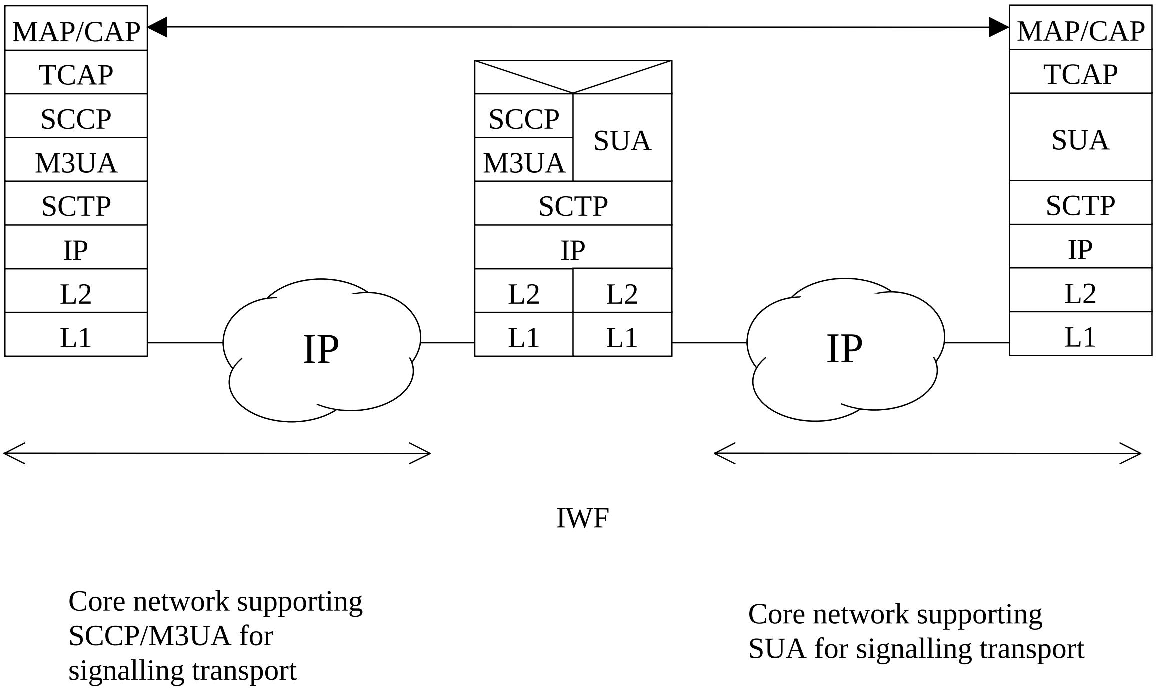
MAP/CAP
TCAP
SCCP
M3UA
SCTP
IP
L2
L1
IP
SCCP
M3UA
SUA
SCTP
IP
L2
L2
L1
L1
IP
MAP/CAP
TCAP
SUA
SCTP
IP
L2
L1
IWF
Core network supporting SCCP/M3UA for signalling transport
Core network supporting SUA for signalling transport

Figure 5: SUA and M3UA interworking with IWF

7.3.2 Global Title management

GTT is done at the SCCP layer of the IWF.

7.3.3 Message Segmentation

Since both M3UA and SUA use SCTP, message fragmentation can be handled at the SCTP layer. See section 7.1.5 for more detail.

8 Services Impact

As discussed earlier in thisdocument, SUA fully supports TCAP, and hence CAP and MAP protocols are supported. Therefore, any applications that use either MAP or CAP protocol (e.g. SMS, CAMEL, etc) shall not be impacted by using the SUA protocol in the core network.

8.1 SMS

The SMS provides a means of transferringshort messages between a GSM/UMTS MS/UE and a SM-SC, and passing through the SMS-GMSC/SMS-IWMSC and the BSS. Mobile Terminated (MT) messages are sent from the SM-SC to the SMS-GMSC; the SMS-GMSC queries the HLR for the location of the MS and forwards the message to the MSC/SGSN which then delivers it to the appropriate BSS and MS. Mobile Originated (MO) messages are sent from the MS to the BSS, the BSS sends the messages to its MSC/SGSN, the MSC/SGSN passes the messages to the SMS-IWMSC, which delivers the messages to the SM-SC. In order to notify that an MS is ready to receive a Short Message, signaling traffic occurs between the MSC/SGSN and the HLR, and is passed over to the SM-SC via the SMS-GMSC/SMS-IWMSC.

SMS utilises several MAP messages and procedures to provide the service. As discussed earlier in the document, SUA fully supports TCAP and hence MAP protocol as a TC-user is supported. Therefore, the SMS service shall not be impacted by implementing the SUA protocol in the core network.

8.2 CAMEL

CAMEL is a service for including IN (Intelligent Network) functions in a GSM/UMTS system, and is provided based on the CAMEL Application Protocol (CAP). CAP is a ROS Element (ROSE) user protocol (see CCITT Recommendation X.219 and CCITT Recommendation X.229). The ROSE protocol is contained within the component sublayer of Transaction Capabilities Application Part (TCAP) (see ETS 300 287-1) and Digital Subscriber Signalling System No One (DSS1) (ITU-T Recommendation Q.932).

The CAP application layer protocol defined in 3GPP TS 29.078, is a protocol thatprovides communication between a pair of application processes. In the SS7 environment this is represented as communication between a pair of application-entities (AEs) using the TC. The function of an AE is provided by a set of application-service-elements (ASEs). The interaction between AEs is described in terms of their use of the services provided by the ASEs.

As discussed earlier in thisdocument, SUA fully supports TCAP and hence CAP protocol as a TC-user is supported. Therefore, the CAMEL service shall not be impacted by implementing the SUA protocol in the core network.

8.3 CCBS

Supplementary Service Application Part (SSAP) is the protocol used for CCBS procedures on the interface between the originating and destination network. Communication across this interface is performed using SCCP Connectionless Signalling.

In GSM networks, the CCBS functionality is distributed across several network entities (see GSM 03.93) including the HLR, VLR, MSC and the MS. The HLR shall provide any necessary signalling interworking between the MAP protocol for call completion services on the MAP D-interface (between the VLR and the HLR) and ISDN CCBS-ASE protocol between the originating and destination networks.

The MAP protocol for CCBS service is specified in TS 29.002. The ISDN CCBS-ASE protocol is specified in ETS 300 356-18. This specification clarifies the interworking within the HLR between these protocols.

CCBS utilises MAP-D and SSAP protocols to provide the service. As discussed earlier in the document, SUA fully supports TCAP and hence MAP and SSAP protocols as a TC-user are supported. Therefore, the CCBS shall not be impacted by implementing the SUA protocol in the core network.

8.4 Mobile Number Portability

Mobile Number Portability (MNP) is the ability for a UMTS or GSM mobile subscriber to change the subscription network within a portability domain while retaining the original MSISDN(s).

North American GSM Number Portability (NAGNP) is the ability for a subscriber to change subscription between North American GSM networks and other subscription networks within a regulated geographical area within North America.

MNP uses MAP protocol to provide the service. As discussed earlier in thisdocument, SUA fully supports TCAP and hence MAP protocol as a TC-user is supported. Therefore, the MNP service shall not be impacted by implementing the SUA protocol in the core network.

9 Security

SUA could be protected by IPsec at the IP layer. The application of IPsec for native IP protocols is defined in TS 33.200 “Network Domain Security” (see [4]), where the protection of MAP over SS7 is separately defined at the application layer.

For SUA, it is reasonable to assume that all the network entities are IP capable. We can further assume that each network entity is able to negotiate security associations with its intra-domain peer by Internet Key Exchange (IKE) protocol. The negotiation and management of inter-domain security association for SUA should align with the specifications in TS 33.200 for native IP protocols.

Compared with MAP over SS7, the security of SUA is enhanced in the sense that a security association will be established for especiallyone peer in one direction. Network wide security associations as they have been used for MAP over SS7 will be used for all the peers between tow given networks. If any peer happens to use the security association in an improper way and to weaken it, then all the protection for the communications between the two networks during the lifetime of the network wide security association may be jeopardized.

In IETF RFC 2719 “Framework Architecture for Signaling Transport” (see [10]), it was suggested to use IPsec to protect the signaling at the IP layer. It was pointed out that “it is recommended that IPsec or some equivalent method be used, especially when transporting SCN signalling over public Internet.”

A recent IETF internet draft “On the Use of SCTP with IPsec”(see [11]) described functional requirements for IPsec and IKE to facilitate their use for securing SCTP traffic. It further addressed the detailed IPsec extensions to cope with multiple destination addresses used in SCTP for a given Security Association (SA).

Therefore, using IPsec to protect SUA is consistent with SCTP specifications in IETF.

Meanwhile, the COOKIE mechanism for SCTP provides extra security.

10 Comparison of SUA and SCCP/M3UA

Generally speaking, the protocol stack based on SUA is less complex and more efficient compared to the protocol stack based on SCCP and M3UA. Consequently, SUA can enhance the efficiency of the core network and can provide the means for simpler implementations.

In an all IP environment, SUA offers significant advantages over M3UA. To illustrate this, we will consider a case, where the SCCP user protocol only knows about the mobile number (E.212 in case of registration) and relies on the underlying protocol to send the message to the IP node associated with that mobile. Also for simplicity, it is assumed that the originating node has access to all the information required to convert the mobile address to a service-specific IP address (Intra-PLMN case). In the figure below, comparison between SUA and M3UA stacks is achieved by comparing the steps involved in finding the peer signalling end point’s IP address. Note that in case of M3UA, to find the IP address of a peer signalling end point, located in a different network, the information should be made available to the layers (SCCP and M3UA) through the mapping tables created by the network craftspeople.

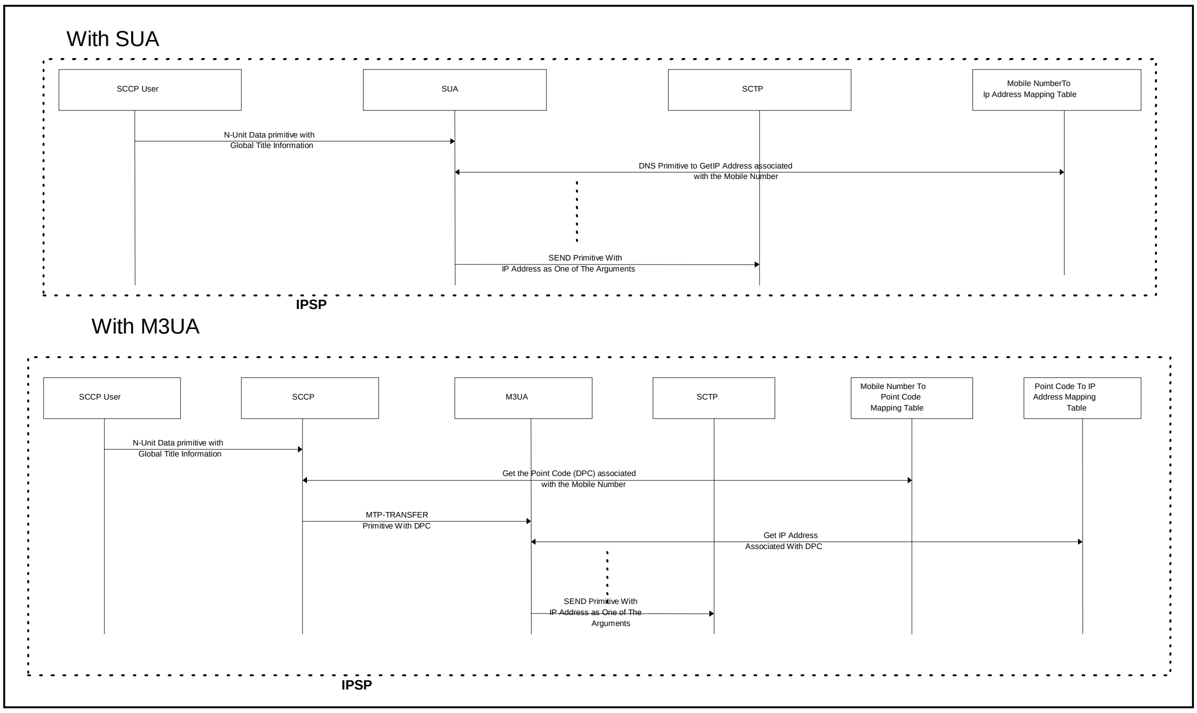
With SUA
SCCP User
SUA
SCTP
Mobile NumberTo Ip Address Mapping Table
N-Unit Data primitive with Global Title Information
DNS Primitive to GetIP Address associated with the Mobile Number
SEND Primitive With IP Address as One of The Arguments
IPSP
With M3UA
SCCP User
SCCP
M3UA
SCTP
Mobile Number To Point Code Mapping Table
Point Code To IP Address Mapping Table
N-Unit Data primitive with Global Title Information
Get the Point Code (DPC) associated with the Mobile Number
MTP-TRANSFER Primitive With DPC
Get IP Address Associated With DPC
SEND Primitive With IP Address as One of The Arguments
IPSP

Figure 6: Transferring SCCP User messages to the peer IP node using SUA and M3UA

As shown in the above figure, even for the most common case (Intra-PLMN), using M3UA:

a) Requires management of two mapping tables to find out the IP address of the peer signalling end point (Adds complexity).

b) Requires two lookups, one to map the mobile number to the point code and another to map the point code to the IP address (Adds processing delay).

c) Requires SCCP node to be configured with both the point code and the IP address (Adds cost to purchase both point code and IP address).

d) With SCCP, it is not possible to use standard IP name services such as ENUM for managing the mapping tables (Mobile number to Point code and point code to IP address).

e) Cannot utilise the IP routing capabilities to send the message to destination IP node without maintaining network wide data locally. So most of thetime, messages are sent hop by hop.

Apart from the drawbacks discussed above, there are other open issues that need to be addressed with M3UA in an inter-PLMN environment, such as availability of point codes, especially if every SCCP node in the IP network requires a unique point code. Recall with SUA, the signalling points do not require a point code.

11 Benefits and Drawbacks

Benefits:

- With M3UA, the signalling point is required to support different flavours of SCCP if it has to inter-operate with different national systems. This problem is eliminated with SUA.
- One less protocol layer with elimination of SCCP reduces the complexity of the network node (implementation as well as management) therefore saves cost.
- SUA allows the IP network to route the messages. This is an advantage of SUA (routed) over M3UA (Point to Point) as M3UA needs to be routed on point codes, while SUA messages can be routed using IP addresses.

- SUA provides much better scalability and flexibility for signalling network implementation in all IP network compared to the SCCP/M3UA option.
- The powerful addressing and routing capability of SUA can greatly reduce the signalling transfer latency.
- With M3UA each IP node is required to have both the IP address and Point Code assigned to it. With SUA each IP node does not consume scarce point code resources.
- With SUA the central-administrated and dynamically updated address mapping data can reduce operator's operation, administration and maintenance costs.
- SUA can provide a smoother migration path to an all IP architecture network providing the introduction of ENUM service.
- SUA combined with ENUM can provide much richer features and services than SCCP/M3UA, such as interworking with SIP based multi-media services.
- The capabilities of SUA, in many cases, may make SCCP and M3UA unnecessary and SUA can be considered preferable in terms of efficiency and implementation complexity.
- IPSec can be used as a general mechanism to protect MAP and CAP messages.

Drawbacks:

- New network nodes such as ENUM server might need to be introduced.

12 Open Issues

- ENUM service deployment: How to deploy ENUM service is an implementation dependent issue. When data retrieving across PLMNs is required, the DNS data administration should be mutually agreed upon by the operators who signed roaming agreements.
- For using IPsec to protect SUA, the following open issues needfurther study: whether both IPsec transport mode and IPsec tunnel mode are applicable to SUA or only one mode. It may depend on the version of IP protocol to be used and maybe other network configuration issues.

13 Conclusion

Based on the SUA advantages and the analysis provided in this technical report, and because many operators have expressed preference for SUA, it is proposed that SUA for IP-based MAP and CAP transport be used as an option in the 3GPP core network.

14 Work Plan

[Editor's note: The work plan will be completed/updated as required as the feasibility study progresses.]

CN4#8	May 14-18, 2001	Presentation of the TR to CN4 for approval.
CN4 workshop	June 05-07, 2001	Solve major outstanding issues and finalise the TR if needed.
CN#12	June 18-22, 2001	Presentation of the final TR to CN for approval.

Appendix A (informative): Mapping between IP address and E.164 (ENUM)

ENUM is one of the mechanisms to put E.164 numbers into the global domain name system (DNS). The ENUM working group in IETF was created to solve the problem of using the DNS for deriving URL (e.g. mailto, sip, http or other URL scheme) from Domain name (reformatted E.164 numbers as domain names).

ENUM allows the IP node to use DNS to discover services connected to an E.164 number. This is accomplished by storing the E.164 number, as specified in RFC 2196, in DNS as a domain name. When wildcards are used, the domain name represents a group of E.164 numbers. Through transformation of E.164 numbers into domain names and the use of NAPTR records in DNS, one can look up the services available for a specific domain name in a decentralised way. Following examples describe how DNS can be used to store information connected to E.164 numbers.

Example 1:

```
;;  Domain Name                                   order pref flags service regexp replacement

$ORIGIN *.6.7.9.8.6.4.e164.arpa. IN NAPTR 10    10   “A”     “”       “”     hlra.plmn10.com

hlra.plmn10.com A 170.10.10.18
```

In the above example all E.164 numbers that start with 468976 are served by hlra.plmn10.com node whose IP address is 170.10.10.18

Appendix B (informative): Document History

Document history		
V0.0.0	2001-03	Document created
V0.1.0	2001-05	Presented at CN4#08 in Puerto Rico
Editor for 3GPP CN4 TR 29.903 is:		
Name: Michael Young Company: Motorola Tel.: +1 604 241-6032 Fax : +1 604 241-6042 Email : michael.young@motorola.com		
This document is written in Microsoft Word 2000.		